Express Mail Label No. EL080833155US 04-04-00 A

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. 96-059-1

Total Pages in this Submission 78

04/03/00 C688 U.S. PTO

jc682 U.S. PTO 09/542676 04/03/00

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER

and invented by:

Jay S. WALKER; Bruce SCHNEIER; Sanjay K. JINDAL; and Daniel E. TEDESCO

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☐ **Continuation** ☒ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: **08/919,339**

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having **36** pages and including the following:
   - a. ☒ Descriptive Title of the Invention
   - b. ☒ Cross References to Related Applications *(if applicable)*
   - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   - d. ☐ Reference to Microfiche Appendix *(if applicable)*
   - e. ☒ Background of the Invention
   - f. ☒ Brief Summary of the Invention
   - g. ☒ Brief Description of the Drawings *(if drawings filed)*
   - h. ☒ Detailed Description
   - i. ☒ Claim(s) as Classified Below
   - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
96-059-1
Total Pages in this Submission
78

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
   a. ☒ Formal Number of Sheets 17
   b. ☐ Informal Number of Sheets
4. ☒ Oath or Declaration
   a. ☐ Newly executed *(original or copy)* ☐ Unexecuted
   b. ☒ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
   c. ☒ With Power of Attorney ☐ Without Power of Attorney
   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Computer Program in Microfiche *(Appendix)*
7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
   a. ☐ Paper Copy
   b. ☐ Computer Readable Copy *(identical to computer copy)*
   c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☐ Assignment Papers *(cover sheet & document(s))*
9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
10. ☐ English Translation Document *(if applicable)*
11. ☒ Information Disclosure Statement/PTO-1449 ☒ Copies of IDS Citations
12. ☒ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☒ Certificate of Mailing
    ☐ First Class ☒ Express Mail *(Specify Label No.):* EL080833155US

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
96-059-1
Total Pages in this Submission
78

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☒ Additional Enclosures *(please identify below):*

Copy of Revocation and Power of Attorney filed on 8/19/99.

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra		Rate	Fee
Total Claims	6	- 20 =	0	x	$18.00	$0.00
Indep. Claims	5	- 3 =	2	x	$78.00	$156.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$690.00
OTHER FEE *(specify purpose)* _____						$0.00
					TOTAL FILING FEE	$846.00

☐ A check in the amount of to cover the filing fee is enclosed.

☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **50-0271** as described below. A duplicate copy of this sheet is enclosed.

- ☒ Charge the amount of **$846.00** as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Signature

Dated: April 3, 2000

Kurt M. Maschoff
Attorney for Applicants
PTO Reg. No. 38,235
Walker Digital Corporation
Five High Ridge Park
Stamford, CT 06905
(203) 461-7020 / Phone

22927
PATENT TRADEMARK OFFICE

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: WALKER et al.	Group Art Unit: 2764 (Anticipated)
Customer No.: 22927	Examiner: D. Smith (Anticipated)
Application No.: Not yet assigned	Attorney Docket No. 96-059-1
Filed: April 3, 2000	Walker Digital Corporation Five High Ridge Park Stamford, CT 06905-1325 (203) 461-7020 / phone (203) 595-8266 / fax
For: METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER	

Box Patent Application
Assistant Commissioner for Patents
Washington D. C. 20231

TRANSMITTAL LETTER

Sir:

Applicants hereby submit the following documents for the above-identified patent application:

1. Certificate of Express Mailing no. EL080833155US;
2. Divisional Patent Application Transmittal (Large Entity) (in duplicate);
3. Copy of Patent Application (36 pages);
4. Set of Formal Drawings (17 sheets: Figs 1-14);
5. Preliminary Amendment;
6. Copy of Combined Declaration and Power of Attorney;
7. Copy of Revocation and Appointment of Power of Attorney;
8. Information Disclosure Statement;
9. PTO-1449 with copies of references cited (23); and
10. Acknowledgment Postcard

The Assistant Commissioner is hereby authorized to charge the associated fee in the amount of $846.00 to Deposit Account No. 50-0271. Order No. 96-059-1. The Commissioner is further authorized to charge any additional fees which may be required for the submission of this paper, or to credit any overpayment, to Deposit Account No. 50-0271. Order No. 96-059-1. A duplicate copy of this authorization is attached for such purpose.

Respectfully submitted,

April 3, 2000

Kurt M. Maschoff
Attorney for Applicants
PTO Reg. No. 38,238
Walker Digital Corporation
Five High Ridge Park
Stamford, CT 06905
(203) 461-7020 / phone
(203) 595-8266 / fax

Certificate of Express Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service via Express Mail in an Envelope No. EL080833755US with sufficient postage addressed to Assistant Commissioner for Patents, Washington, DC 20231 on April 3, 2000.

Jill Doherty
Typed Name of Person Making Deposit

Signature

04/03/2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: WALKER et al.

Customer No.: 22927

Application No.: Not yet assigned

Filed: April 3, 2000

For: METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER

Group Art Unit: 2764 (Anticipated)

Examiner: D. Smith (Anticipated)

PRELIMINARY AMENDMENT

Attorney Docket No. 96-059-1

Walker Digital Corporation
Five High Ridge Park
Stamford, CT 06905-1325
(203) 461-7020 / phone
(203) 595-8266 / fax

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail under Express Mail No. EL080833753US" under CFR 1.10 in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on April 3, 2000.

Dated: April 3, 2000 By: Jill Doherty

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Before examination of the above-identified application, and before calculation of any fees, please amend the above-identified application as follows:

At page 1, before the first full paragraph, please insert:

--CROSS REFERENCE TO RELATED APPLICATIONS

This application is a divisional of U.S. Patent Application Serial No. 08/919,339 entitled "METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER" filed in the name of Jay S. WALKER; Bruce SCHNEIER; Sanjay K. JINDAL; and Daniel E. TEDESCO on August 28, 1997. --

IN THE CLAIMS

Kindly cancel claims 1-14, 17, 20-22, 24, and 26-27 without prejudice.

REMARKS

The Examiner has issued a restriction requirement in the patent application, in response to which applicants have elected group I for prosecution. The applicants have filed this amendment to pursue claims, 16, 19, 23, 25, 28 and 29, representing the Examiner's group II.

If there are any issues that remain, or if the Examiner has suggestions for expediting allowance of the present application, the Examiner is kindly invited to contact Kurt Maschoff at telephone number (203) 705-7020 or via electronic mail at Kurt.Maschoff@WalkerDigital.com.

Please charge any additional fees that may be required for this Amendment, or credit any overpayment to Deposit Account No. 50-0271. A copy of this authorization is included for such purpose.

Entry of this amendment is respectfully requested.

Respectfully submitted,

April 3, 2000
Date

Kurt M. Maschoff
Attorney for Applicants
Registration No. 38,235
Walker Digital Corporation
Five High Ridge Park
Stamford, CT 06905-1326
(203) 461-7020 / phone
(203) 595-8266 facsimile

16. An apparatus for verifying a second account identifier for use in place of a first account identifier, comprising:

a processing unit, said processing unit including a cryptographic processor;

a communications unit, connected to said processing unit, operable to transmit and receive information regarding a second account identifier for use in place of a first account identifier; and

a memory device connected to said processing unit, said memory device containing

a private cryptographic key,

a first data element,

a second data element and

a program, adapted to be executed by said processing unit, to

receive the second account identifier,

extract from the second account identifier a third data element and a fourth data element,

decrypt the third data element using the private cryptographic key and the fourth data element,

compare the decrypted third data element with the first data element in a first comparison,

compare the fourth data element with the second data element in a second comparison, and

verify the second financial account identifier in accordance with the first comparison and the second comparison.

19. A method for verifying a second account identifier for use in place of a first account identifier, comprising the steps of:

providing a memory device containing a private cryptographic key, a first data element and a second data element;

receiving a second account identifier;

extracting from the second account identifier a third data element and a fourth data element;

decrypting the third data element using the private cryptographic key and the fourth data element;

comparing the decrypted third data element with the first data element in a first comparison;

comparing the fourth data element with the second data element in a second comparison; and

verifying the second account identifier in accordance with the first comparison and the second comparison.

23. An apparatus for verifying a second account identifier for use in place of a first account identifier, comprising:

a processing unit;

a communications unit, connected to said processing unit, operable to transmit and receive information regarding a second account identifier; and

a memory device connected to said processing unit, said memory device containing

data representing a plurality of predetermined account identifiers,

data representing a status for each of said plurality of predetermined account identifiers, and

a program, adapted to be executed by said processing unit, to

receive said second account identifier,

compare said second account identifier with at least one of said plurality of predetermined account identifiers to identify one predetermined account identifier matching said second account identifier, and

verify said second account identifier in accordance with said comparing step and the data representing the status of said one predetermined account identifier.

25. A method for verifying a second account identifier for use in place of a first account identifier, comprising the steps of:

providing a memory device containing

data representing a plurality of predetermined account identifiers and

data representing a status for each of said plurality of predetermined account identifiers;

receiving a second account identifier;

comparing said second account identifier with at least one of said plurality of predetermined account identifiers to identify one predetermined account identifier matching said second account identifier; and

verifying said second account identifier in accordance with said comparing step and the data representing the status of said one predetermined account identifier.

28. A method for verifying a second account identifier for use in place of a first account identifier, comprising the steps of:

receiving a plurality of second account identifiers, each second account identifier being different from remaining second account identifiers; and

verifying that each of the plurality of second account identifiers indicates a first account identifier.

29. The method of claim 28, in which the first account identifier and each second account identifier respectively comprise sixteen digits.

METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER

BACKGROUND OF THE INVENTION

This invention relates to a method and a device for generating a single-use, transaction-specific financial account number, thereby providing a high level of security for financial transactions, particularly credit card transactions.

There are over 500 million general purpose, retail, oil and other credit card accounts in the United States (hereafter called "cards"). Worldwide the figure is almost 1 billion such cards. Typically, each authorized user of an account is issued a credit card: a physical plastic object with an embossed account number and cardholder name appearing on its face. Anti-counterfeiting indicia, such as holograms, photographs or signatures, may also appear on the card to discourage wrongful usage.

Since the credit card number is unchanging, there is a risk of fraudulent use by anyone who steals the number. The key element of defense against a fraudulent user impersonating the authentic cardholder is signature verification. A signature area appears on the back of most cards, and when a person receives a new credit card, he is instructed to sign his name on the back of the card. A merchant who accepts the card will then be able to compare the signature specimen that

appears on the back of the card to the signature on the sales draft signed by the consumer at the time of purchase. In some cases, the merchant may also ask for photo ID before accepting the card or as a method of checking that the signatures are for the person whose name appears on the face of the card.

In addition to examining the signature on the card, most merchants who accept credit cards use a small device known as an authorization terminal. The authorization terminal is capable of reading information disposed on a magnetic stripe located on the back of the credit card. In some cases, this stripe also contains other difficult-to-counterfeit information. To process a credit card purchase, the merchant passes the card through the magnetic stripe reader of the terminal and enters the amount of the purchase. The information is then sent by the device over a phone or wireless connection to a central database for account number verification and purchase authorization. A card that has been reported lost or stolen is declined. If magnetic stripes on credit cards become damaged and unreadable, the authorization terminal permits manual entry of the credit card number as it appears embossed on the face of the card.

With the dramatic growth of direct marketing, an increasing share of all card purchases are being made without the physical presentation of the card to the selling merchant. Instead, the consumer simply relays the card number to the merchant, and the merchant enters the card number into a computer terminal which is also designed to handle the order processing function. As electronic commerce grows over the next decade, the percentage of such remote, non-face-to-face purchases can be expected to grow. This poses an increasingly acute problem for the entire credit card system,

since credit card numbers are highly insecure.

To protect against thieves fraudulently creating credit card numbers and then using them for remote purchasing, a check-digit algorithm is typically employed for credit card account numbers which makes it comparatively difficult (approximately 1 chance in 500,000) to pick a random 16-digit number that is also a valid credit card account number. In addition, since not every valid credit card account number is currently in use, simply making up a valid number is, in itself, not enough to get an authorization code from the central authorizing network. In addition to passing the check-digit test, a bank must have issued that number to an active customer.

To further help combat mail-order based credit card fraud, both Visa and MasterCard have deployed databases that allow a merchant to verify that a given credit card account number is connected to a specific billing address. Visa calls this service the Address Verification Service. The theory behind the service is that a thief (for example, a dishonest restaurant waiter) might be able to use a credit card receipt slip to steal an active account number, but if he tries to use that number for a mail order purchase he would not know the correct address associated with that number. Even if a thief were to obtain the cardholder's address, this service can allow a merchant to compare the shipping address of the catalog order to the current billing address for that account number and thus possibly identify any suspicious activity.

Currently, credit cards also incorporate an expiration date after which they are no longer valid. These dates are typically one to two years after the card is issued. The reason for an expiration date is to reduce the issuing bank's

risk of cards being presented after an account is closed. Since the expiration date is an absolute indication of whether or not to accept a card, an old card that is lost or misplaced eventually expires with minimal risk that it will be found and used improperly.

In addition, credit card information and transaction information may be encrypted using well known encryption schemes like RSA's public key cryptography. For example, SET is a joint Visa/MasterCard standard for encrypting credit card numbers transmitted over the Internet.

In spite of these safeguards, credit card security is vulnerable to a number of attacks by unscrupulous persons. Some examples of these attacks are as follows:

a) Theft of cards: Any conventional credit card which is stolen can be misused, either at a merchant's establishment by forging the signature on the card onto a sales slip, or by ordering merchandise or services remotely.

b) "Sniffing:" Credit card transaction information being transmitted over public networks can possibly be intercepted and captured or "sniffed." The sniffed information can then be used to create counterfeit cards and/or order goods and services. For example, if a hacker were to break the SET encryption scheme, the hacker could sniff out credit card numbers and misuse them. Re-submission of the sniffed encrypted credit card numbers to the same merchant is known as "replay."

A large-scale attack on credit-card number security would threaten the entire credit card system. For example, if someone were to steal 1 million active credit card account

numbers, and were also able to steal the billing addresses to which those cards were issued, the entire credit card system would be threatened. At the very least, mail order sales might have to be suspended until new safeguards were put in place. At worst, a flood of counterfeit cards, with correct account numbers and valid names embossed on their faces, could be created.,

With the advent of almost instantaneous worldwide money transfers, a band of organized thieves could clear hundreds of millions or even billions of dollars of charges through the authorization system and then wire that money to a safe haven before cardholders suspected that their cards had been charged an unauthorized amount. If the theft also involved data revealing each account's unused available credit line, such criminal activity might be even harder to detect before it was too late to rescind the wire transfers of stolen money.

Cards which store information, as opposed to merely having embossed numbers, are known in the art. Such "smart cards" are becoming increasingly common. These cards contain a small microprocessor capable of storing data in a secure fashion and of performing computer operations on such data. Smart cards may have built-in small numeric display screens. In particular, smart cards used for distribution of cryptographic keys, display keys on their display screens.

Smart cards are used to authenticate card users and to authenticate the card/user combination to a third party. These cards are also used for controlling access to computer systems and databases and entry into secure areas. Northern Telecom offers a credit card sized smart card called Entrust which contains a microchip that stores encoded, private keys.

Hardware tokens such as Security Dynamics' SecurID card use a "time synchronous methodology" to produce passwords every 30 seconds.

Wire transfer calculator-style devices are also known in the art. Such devices are the size of a credit card and contain a tamper-resistant, "secure perimeter" within which is disposed a clock and a cryptoprocessor. These devices also have a small LCD alpha-numeric display screen and a numeric keypad for data entry.

A number of security devices and methods involving credit cards have been disclosed. For example, U.S. Patent No. 5,311,594, "Fraud Protection For Card Transactions," describes a challenge-response method for fraud protection wherein credit card holders are authenticated based on their responses to randomly asked questions like their mother's phone number, their graduation year, birth date, etc. The responses are checked against prestored information in a database.

U.S. Patent No. 5,457,747, "Anti-Fraud Verification System Using a Data Card," describes a biometric system for deterring credit card fraud. Credit cards have two magnetic stripes, one that has been permanently encoded with the card holder's biometric information and one that an ATM can write onto. To use the card, the card holder supplies the same biometric information at a verification terminal. The terminal checks the biometric information supplied by the card holder against that recorded on the magnetic stripe. If the biometrics match, the terminal will write a transaction authorization onto the magnetic stripe.

U.S. Patent No. 5,485,519, "Enhanced Security For a Secure

Token Code," describes a method for enhancing security for a private key stored in a smart card. A user input PIN is combined algorithmically with a code resident in the smart card to produce the private key. The private key is not stored in the smart card except for short intervals when the card is actually being used by an authorized user who has input his PIN.

SUMMARY OF THE INVENTION

This invention provides a method and a device to facilitate secure electronic commerce, secure remote credit card purchases, and secure conventional credit card purchases wherein the customer is assured that the merchant or an intercepting third party cannot misuse any credit card information.

According to one aspect of our invention, a method for generating a single-use financial account identifier is provided which includes the steps of accessing a first data element specific to an account; accessing a second data element including transaction-specific data; and combining the first data element and the second data element to produce the single-use financial account identifier.

According to another aspect of our invention, a device for facilitating credit transactions is provided which includes a processing unit including a cryptographic processor. The device also includes an input unit connected to the processing unit for inputting information thereto, and a display unit connected to the processing unit for displaying a processing result. In addition, the device includes a memory device connected to the processing unit. The memory

device contains a private cryptographic key, a first data element, a second data element and a program adapted to be executed by the processing unit. In accordance with the program, the processing unit encrypts the first data element using the private cryptographic key and the second data element, modifies the second data element, combines the encrypted first data element and the second data element to generate a single-use financial account identifier, and displays the single-use financial account identifier using the display unit.

According to a further aspect of our invention, a system for verifying a financial account identifier is provided which includes a processing unit including a cryptographic processor. The system also includes a communications unit, connected to said processing unit, for transmitting and receiving information regarding the financial account identifier, and a memory device. The memory device contains a private cryptographic key, a first data element, a second data element and a program adapted to be executed by the processing unit. In accordance with the program, the processing unit receives a single-use financial account identifier, extracts therefrom a third data element and a fourth data element, decrypts the third data element using the private cryptographic key and the fourth data element, compares the decrypted third data element with the first data element in a first comparison, compares the fourth data element with the second data element in a second comparison, and verifies the received financial account identifier in accordance with the first comparison and the second comparison.

According to still another aspect of our invention, a method for providing a single-use financial account identifier

includes the steps of: providing a memory storing data representing a plurality of predetermined single-use financial account identifiers, data representing a status for each single-use financial account identifier, and data representing a pointer to one of the single-use financial account identifiers; identifying the single-use financial account identifier based on the pointer data; and transmitting a signal to an output device to present the single-use financial account identifier.

According to a further aspect of our invention, a device for providing a single-use financial account identifier is provided which includes a memory, an output device and a processor coupled to the memory and to the output device. The memory stores data representing a plurality of predetermined single-use financial account identifiers, data representing a status for each of the predetermined single-use financial account identifiers, and data representing a pointer to one of the predetermined single-use financial account identifiers. The output device presents the single-use financial account identifier. The processor is configured to identify the single-use financial account identifier based on the data representing a pointer, and to transmit a signal to the output device to present the single-use financial account identifier.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of the hand-held smart card device in accordance with the present invention.

Figure 2 is a block diagram of the device's central processor.

Figure 3A is a block diagram of the overall system of the present invention.

Figure 3B is a flowchart showing the basic method of the present invention.

Figure 4 is a block diagram of the credit card issuer's central processor, with databases as used in accordance with the first embodiment of the invention.

Figure 5 shows in tabular form the credit card account holder database.

Figure 6 shows in tabular form the account holder secret key database.

Figure 7 shows in tabular form the credit card transaction database according to the first embodiment of the invention.

Figure 8 is a flowchart describing an encryption scheme used to generate a single-use credit card number in accordance with the first embodiment of the invention.

Figures 9A and 9B are connected flowcharts describing the operations performed by the central processor of a credit card issuer to generate an authorization code, in accordance with the first embodiment of the invention.

Figure 10 is a flowchart describing the operations performed by a device to generate and display a single-use credit card number, in accordance with a second embodiment of the invention.

Figures 11A and 11B are connected flowcharts describing the operations performed by a credit card issuer's central controller to generate an authorization code, in accordance with the second embodiment of the invention.

Figure 12 is a block diagram of the credit card issuer's central processor„ with databases as used in accordance with the second embodiment of the invention.

Figure 13 shows in tabular form the credit card number database.

Figure 14 shows in tabular form the credit card transaction database according to the second embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 is a schematic diagram of a device 100 for generating a single-use credit card number in accordance with this invention. This device is preferably a smart card, hereinafter referred to as the "device." The device has a keypad 103, a display screen 102, a memory 104 and a central processor 101. Memory 104 contains a key 601, and CPU 101 contains a cryptographic processor. The device may be activated through the input of a unique cardholder identifier such as a personal identification number (PIN) through the keypad 103. Alternatively, the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint.

Figure 2 is a schematic diagram showing further details of the central processor 101 of device 100. The central

processor 101 includes a microprocessor 201. The microprocessor 201 is connected to a clock 202, a random-access memory (RAM) 203, a read-only memory (ROM) 204, and a cryptographic processor 205. In addition, the microprocessor 201 is connected to the keypad 103 for receiving input from the user and to the display 102 for prompting the user or displaying information.

Figure 3A is a schematic diagram of the environment in which the method and system of the present invention are used. A cardholder 301, wishing to purchase goods or services from a merchant 302 (not necessarily in person), transmits a single-use credit card number 300 to the merchant. The merchant 302 transmits the single-use credit card number 300 to a credit card issuer 303. The credit card issuer 303 returns an authorization 310 to the merchant, based on which the merchant delivers the desired goods or services 320 to the cardholder.

Figure 3B shows the steps of the basic method of using the device in accordance with the present invention. To purchase goods or services in person, via telephone or via the Internet, cardholder 301 uses device 100 to generate a transaction-specific, single-use credit card number. The cardholder first inputs his PIN or biometric data to access the device (step 351). If access is granted, the device responds by querying the cardholder on display 102 whether it should generate a single-use credit card number (step 355). The cardholder responds by requesting generation of a credit card number (for example, by keying "YES"). He may optionally be asked to enter the amount of the purchase in step 356 or a merchant code number provided by the merchant. This number could be only a few digits long since it does not have to be unique to each merchant.

The device then generates a single-use credit card number (step 360); details of the card number generation are explained below. The number is unique for the specific input variables set by the cardholder or by the device. It may also be unique to the specific date and time to avoid so-called "replay" attacks for that card at that merchant with that exact purchase amount. The single-use credit card number is preferably a 16-digit number that can be recognized as a conventional credit card number.

The cardholder transmits the single-use number to the merchant (step 361), and the merchant enters the single-use number into an authorization terminal connected to a central credit card processing system maintained by the credit card issuer (step 362). A check digit may be included in the number to prevent the incorrect keying of the number. The number is sent to the credit card processing system for authorization (step 363). The central system processor maps the single-use credit card number onto a conventional credit card account and determines whether the transaction is authorized (step 380); if so, the central system returns an authorization code for display on the merchant's authorization terminal (step 390); if not, the central system transmits an authorization failed message for display on the merchant's authorization terminal (step 395).

Throughout this discussion, the term "credit card number" refers to a number that is used only one time to perform a specific transaction, and is generated using the device 100; in contrast, the term "account number" refers to an unchanging identifier for the cardholder which is stored in a database maintained by the card issuer.

First Embodiment (Device Private Key Encryption)

In this embodiment, the single-use credit card number is generated by the device cryptoprocessor 205, using a private key 601 stored in the device memory 104 (preferably the ROM 204). The encryption data changes with each use of the card, so that the single-use encrypted credit card number is different for each transaction. This credit card number is distinct from the unchanging account number identifying the particular cardholder. It should be noted that knowledge of the account number does not allow an attacker to generate a valid single-use credit card number.

When the single-use credit card number is transmitted to a merchant, the merchant passes the number to the card issuer's central processor for authorization. The central processor decrypts the number based on a known algorithm, determines the true account number, and either authorizes or denies the charge.

Figure 4 is a schematic diagram of the credit card issuer's central processor 400. The processor includes a central processing unit (CPU) 401. The CPU is connected to a clock 402, a random-access memory (RAM) 403, a read-only memory (ROM) 404, a cryptographic processor 405, and a communication port 406 for communication with the merchant's central processor. In addition, the CPU 401 is connected to a storage device 410, which includes a credit card account holder database 411, a credit card account private key database 412, and a credit card transaction database 413.

The data structure of the credit card account holder database 411 is shown in Figure 5. Each record in the database

includes the cardholder account number 501, the cardholder's name 502, address 503 and telephone number 504, the original credit line 505 associated with the account, the amount of credit currently available (available credit line 506), and the expiration date 507.

Figure 6 shows the fields of the credit card account private key database 412. Each entry of this database has the cardholder private key 601 and the associated cardholder account number 501. The private key is thus stored in both the device memory 104 and the database 412. An additional secret piece of information, called a "nonce" 602, is associated with the account number. The nonce is also stored in the device memory 104. The nonce need not be as long as the account number, but should not be easily derived therefrom.

Figure 7 shows the fields of the credit card transaction database 413. Each record of this database corresponds to one transaction using the card, and includes the account number 501, the expiration date 507 of the card, the transaction amount 702, the merchant identification number 703 and an initialization variable 704. The initialization variable 704 is used to ensure that each credit card number is unique to the particular transaction, thereby preventing a "replay" attack.

In this embodiment, the device memory 104 has stored therein the private key 601, the nonce 602, the initialization variable 704 and the account number 501. The initialization variable is set at 0 (zero) when the card is newly issued, and is incremented each time a single-use credit card number is generated.

The cryptography described herein requires binary data. Current credit card numbers are 16-digit decimal numbers. Since 10^{16} is only slightly greater than 2^{53}, nearly every such decimal number may be represented by a 53-digit binary number. Therefore, in the following discussion it will be assumed that the credit card number is a 53-bit number and that it is then converted to a 16-digit decimal number for transmission or display.

A credit card number consists of an m-bit initialization variable (abbreviated IV), an a-bit account number, and an n-bit nonce (abbreviated N), where m+a+n = 53. It should be noted that the nonce may take the place of the check code employed with conventional credit card numbers. If n = 16, then the probability that an attacker can generate a valid credit card number is 1 in 2^n = 65536. The parameter n can be varied to change the probability as desired.

The parameters m and a do not necessarily have to be the same size for all credit card holders. However, m should be large enough for any individual cardholder so that he does not use his credit card more than 2^m times before the card expires. For most credit card holders a value of m = 9 would probably suffice, allowing use of the card 512 times (that is, 5 times a week assuming the card is valid for two years) before it expires.

The steps for generating an encrypted single-use credit card number according to this embodiment are shown in Figure 8. In step 801, the device central processor 101 retrieves the nonce 602 and the initialization variable 704 from the device memory 104. In step 802, the nonce is encrypted using the user's private key K and the IV. Thus

$$C = E_K(N, IV)$$

where C represents the encrypted nonce. Both N and C are n-bit values.

The central processor 101 then retrieves the account number from the device memory 104 (step 803). In step 804, the encrypted nonce C, the initialization variable IV, and account number A are concatenated to form an encrypted, single-use credit card number CCN:

CCN = C_IV_A, where _ denotes concatenation.

The initialization variable is incremented and the result is stored in the device memory 104 (step 805):

IV = IV + 1

The resulting credit card number CCN is then displayed on the display screen 102 (step 806) and read, shown or otherwise transmitted to the merchant. The merchant transmits this number to the issuer's central processor 400 for authorization of the transaction.

Figures 9A and 9B show the steps for generating an authorization code for the transaction. In step 901 the issuer's central processor 400 receives the single-use credit card number transmitted by the merchant.

To verify the card number, the credit card issuer's central processor first extracts the encrypted nonce C, the initialization variable IV, and account number A from the credit card number (step 902). The processor then retrieves the extracted account number from the cardholder account database 411 (step 903), and determines whether the account number is valid (step 904). If the account number is not valid, the transaction is aborted (step 905). If the account number is valid, the processor looks up the account number in

the credit card transaction database 413 to determine whether the card holder has previously used the initialization variable IV (step 906). If the cardholder has done so, the transaction is aborted (step 908). If the initialization variable has not been used, the incremented initialization variable is stored in the credit card transaction database 413 (step 908).

In step 921, the processor retrieves the card holder's private key K in the private key database 412. The private key K then is used to decrypt the encrypted nonce (step 922). This recovers the original nonce N:

$$N = D_K(C, IV).$$

The decrypted nonce N is compared against the nonce 602 stored in the account private key database 412 (step 923). If they match (step 924) then the credit card number is considered valid; otherwise the transaction is aborted (step 925).

If the card is found to be valid, and if the cardholder's account meets the credit card issuer's approval criteria (step 926), then the issuer's central processor generates an authorization code and transmits the code to the merchant (step 928). If not, then the transaction is aborted (step 927).

Approval criteria are issuer specific and may include, but are not limited to, the following: account must be in good standing (not past due); sufficient credit must be available (some issuers may approve purchases that exceed available credit by a specified margin), the card should not have been reported stolen/lost; and the account should not be closed.

There are two types of ciphers which can be used to encrypt

the data (in this embodiment, the nonce N and initialization variable IV): stream ciphers and block ciphers. Stream ciphers can be used with minor modification so that different initialization variables will result in different ciphertext. The amount of information that must be encrypted in this system is smaller than the blocksize of most block encryption algorithms. However, a modified variant of Cipher Feedback Mode may be used to encrypt small amounts of data and has some additional security features.

Accordingly, one possible encryption method uses a stream cipher. Conventional ciphers use a secret key k to produce a stream of data. The data is then combined with the unencrypted data (e.g. by XORing them together) to produce the encrypted text. On the other hand, to encrypt an n-bit value N using initialization variable IV and key k, a stream cipher may be used to generate n(IV + 1) bits of data, with N then combined with the last n bits of the resulting data.

Another way to encrypt the data is to use a block cipher in 1-bit feedback CFB-mode. However, this has some undesirable properties which may allow an attacker to deduce the unencrypted form of encrypted data. While an attacker cannot generate a valid credit card number without knowledge of the user's private key, knowing the user's nonce undermines the security of the account. To avoid this problem the following variant may be used:

1. The input of the block cipher I_i consists of the IV concatenated with a 1 - m bit shift register (where m is the number of bits in the IV and we are using a 1-bit block cipher). Let S_i be the state of the shift register. Then

$$S_0 = 1$$

and

$$I_0 = IV\_S_0.$$

In fact, $I_i = IV\_S_i$

for all i.

2. Bit i of the encrypted data is computed as

$$C_i = f(I_i,k)_0 \oplus P_i$$

where f is the encryption function of the block cipher and $f(I/k)_0$ denotes bit 0 of the encryption of I with key k.

3. The shift register is updated with the ciphertext so that

$$S_{i+1} = (S_i<<1)\_C_i$$

where S << 1 denotes shifting S left 1 bit.

To decrypt the data a nearly identical algorithm is used except that P_i and C_i are reversed. So the second step of the algorithm is all that changes and it becomes:

2') Bit i of the decrypted data is computed as

$$P_i = f(I_i,k)_0 \oplus C_i$$

where f is the encryption function of the block cipher and $f(I,k)_0$ denotes bit 0 of the encryption of I with key k.

Suitable block ciphers include Triple-DES, IDEA and Blowfish. Suitable stream ciphers include RC4, SEAL and A5. All of these algorithms are discussed in B. Schneier, "Applied Cryptography," John Wiley & Sons, 2d ed. 1996.

The primary defense against replay attacks in this embodiment is checking that the same initialization variable IV is not used twice for any particular account number. When the credit card is issued the internal IV is preferably set to 0. Each time the credit card is used the IV increments by 1. Therefore, as long as the cardholder does not use the credit card more than 2^m times (where the IV is m bits long) the

same initialization variable will never be repeated. Preferably, the credit card issuer keeps track of the IVs that the card holder has used. This can be done with a simple bit array where entry a of the array indicates that IV a has been used if and only if it is set to 1.

As stated earlier, m = 9 is probably sufficient for most cardholders. This means that the card issuer needs only keep track of a 512-bit array for each such credit card. This is very inexpensive. In addition, if the issuer notices that the cardholder has nearly exhausted his IVs, then it can issue the cardholder a new card.

Another attack against this system would be to flood the central server with bogus credit card numbers (otherwise known as a denial-of-service attack). One way to make this attack more difficult is to spread the authorization processing load across several servers which all have the capability of verifying a credit card number. If they receive a valid credit card number, they can coordinate with the central server to perform the credit card transaction.

Ideally, the load should be spread evenly across several different servers. A simple way to do this is to set up p servers and assign each a unique number in the range 0 to 2^p-1. Next, for every credit card number that must be verified, check a prespecified set of p bits of the credit card number and assign the verification to the server with the corresponding number. For example, if the p specified bits of the credit card number give "14," assign the verification to the server numbered "14."

For the primary embodiment, there are 2^{53} possible credit card numbers. A central authority might be established to assign

ranges of account numbers to individual credit card companies. Once a company receives an r-bit range of account numbers it may further split the range of numbers up as desired. Ultimately the issuer should decide upon the size of the nonce (n bits), the account number (a bits), and the size of the IV (m bits) so that n+a+m = r. Note that the account number should include those bits assigned by the central authority. Also, different card holders can have different values of n, a, and m even if they receive their cards from the same credit card company.

After a cardholder's card expires, his account number can be reused. The next credit card issued with that account number would use a different nonce and private key. This will ensure that any credit card numbers generated with the old credit card will not match any new credit card numbers with better than random chance.

In an alternative to the present embodiment, timestamps could be included with the nonce during encryption. Then, credit cards could be used in conjunction with a clock. When creating the credit card the credit card issuer should start the clock at 0 and note the offset from its own clock, storing the difference with the card holder's account information (for example in the database 411). Then when a credit card issuer desires to validate a timestamp created by the credit card, it may simply add the timestamp to the offset stored with the card holder's account and then compare the result against its own clock. If the time falls within a specified time window then the timestamp should be considered valid.

In order for the credit card issuer to verify a single-use credit card number, it must know to which account the credit

card number belongs. Instead of encoding the account number as part of the credit card number, the name that appears on the card could take the place of the account number. In that case every credit card must have a different name printed on the card. The trade-off in this instance is that many more bits become available in the credit card number since they are not used to encode the account number. They can then be used to encode a timestamp, purchase information, or even merchant information.

Second Embodiment (Lists of Single-Use Credit Card Numbers)

In this embodiment, the device memory 104 includes a database with a list of single-use credit card numbers and a flag for each number indicating whether the number has already been used. The single-use credit card numbers are assigned to the cardholder by the credit card issuer.

One method to assign single-use credit card numbers is as follows. There are 2^{53} possible credit card numbers. Some sort of central authority could assign ranges of account numbers to individual credit card companies. Once a company receives an r-bit range of account numbers they can further split the range of numbers up however they please. Ultimately, the credit card company would decide upon the size of the nonce (N bits), the account number (A bits), and the size of the IV (m bits) so that n+a+m = r. The account number would include those bits assigned by the central authority. Also, different card holders can have different values of n, a, and m even if they received their cards from the same credit card company. It is simply up to the company to keep track of the appropriate information.

After a card holder's card expires their account number can be reused. The next credit card issued with that account number should use a different nonce and private key. This will ensure that any credit card numbers generated with the old credit card will not match any new credit card numbers with better than random chance.

The steps for obtaining a single-use credit card number according to this embodiment are shown in Figure 10. In step 1001, the cardholder enters his unique identifier (for example, a PIN or biometric data) into the device. The device determines whether the identifier is valid for the device (step 1002); if not, access to the device is denied (step 1004). If the identifier is valid, the device searches the single-use credit card number database in the device memory 104 for a single-use credit card number (step 1003). If a single-use credit card number is available (step 1005), it is displayed on the device display screen 102 (step 1007); if not, a message is displayed instructing the cardholder to obtain a new device (with a new list of single-use credit card numbers) from the credit card issuer (step 1006). The database in the device memory 104 is then updated to change the status of the number from "not used" to "used" (step 1008).

A schematic diagram of the credit card issuer's central processor according to this embodiment is shown in Figure 12. The processor 1200 includes a central processing unit (CPU) 1201. The CPU is connected to a clock 1202, a random-access memory (RAM) 1203, a read-only memory (ROM) 1204, and a communication port 1206 for communication with the merchant's central processor, similar to the first embodiment. In addition, the CPU 1201 is connected to a data storage device 1210, which includes a credit card account holder database

1211, a credit card number database 1212, and a credit card transaction database 1213. The credit card account holder database 1211 has the same structure as database 411.

The fields of the credit card number database 1212 are shown in Figure 13. Each cardholder account number 501 is associated with the cardholder name 502 and a list of credit card numbers 1301; each credit card number has associated therewith its status 1302 (used or not used).

The fields of the credit card transaction database 1213 are shown in Figure 14. Each record of this database corresponds to one transaction using the card, and includes the account number 501, the expiration date 507 of the card, the transaction amount 702, and the merchant identification number 703.

The steps for generating an authorization code for a credit transaction in this embodiment are shown in Figures 11A and 11B. In step 1101, the cardholder provides the merchant with a single-use credit card number displayed on the device (see step 1007 of Figure 10). The merchant then transmits the single-use credit card number and the transaction amount to the credit card issuer's central processor 1200 (step 1102). The central processor searches the credit card number database 1212 to identify the account holder of the transmitted single-use credit card number (step 1103), and determines whether the transmitted credit card number matches a credit card number listed in the credit card number database (step 1104). If there is no match, the credit card number is considered invalid, and the transaction is aborted (step 1105). If there is a match, the credit card number is considered valid, and the central processor checks the status 1302 of the credit card number to determine whether the

credit card number has already been used (step 1106). If so, the number is no longer valid, and the transaction is aborted (step 1107).

If the cardholder's account meets the credit card issuer's approval criteria (step 1121), then the issuer's central processor generates an authorization code and transmits the code to the merchant (step 1123). If not, the transaction is aborted (step 1122). Finally, in step 1124, the issuer's central processor changes the status 1302 of the credit card number from "not used" to "used."

While the present invention has been described above in terms of specific embodiments, it is to be understood that the invention is not limited to the disclosed embodiments. On the contrary, the present invention is intended to cover various modifications and equivalent structures included within the spirit and scope of the appended claims.

We claim:

1. A method for generating a single-use financial account identifier, comprising the steps of:

accessing a first data element, specific to an account;

accessing a second data element including transaction-specific data; and

combining said first data element and said second data element to produce said single-use financial account identifier.

2. The method of claim 1 wherein the step of accessing said first data element includes accessing an account identifier.

3. The method of claim 2 wherein said account identifier is alpha-numeric.

4. The method of claim 1 wherein the step of accessing said second data element includes accessing a time.

5. The method of claim 1 wherein the step of accessing said second data element includes accessing a payment amount.

6. The method of claim 1 wherein said step of accessing said second data element includes accessing a merchant identifier.

7. The method of claim 1 wherein the step of accessing said first data element includes encrypting said first data element.

8. The method of claim 7 wherein the encrypting step is based on a private key encryption technique.

9. The method of claim 1 wherein the combining step is based on a hashing function.

10. The method of claim 1 wherein the combining step includes encrypting said first data element and said second data element.

11. The method of claim 10 wherein the encrypting step is based on a private key encryption technique.

12. The method of claim 1, further comprising the step of accessing a third data element including a static account identifier, and wherein said combining step includes combining said third data element with said first data element and said second data element.

13. The method of claim 1, further comprising the step of updating said second data element to initialize for a future transaction.

14. A device for facilitating a financial account transaction, comprising:

a processing unit, said processing unit including a cryptographic processor;

an input unit connected to said processing unit for inputting information thereto;

a display unit connected to said processing unit for displaying a processing result therefrom; and

a memory device connected to said processing unit, said memory device containing a private cryptographic key, a first data element, a second data element and a program, adapted to be executed by said processing unit, to encrypt the first data element using the private cryptographic key and the second data element, modify the second data element, combine the encrypted first data element and the second data element to generate a single-use financial account identifier, and display the single-use financial account identifier using said display unit.

15. An apparatus for facilitating a financial account transaction, comprising:

a processing unit;

an input device connected to said processing unit for inputting a financial account identifier thereto;

a transmitting/receiving device connected to said processing unit for transmitting the financial account identifier for verification thereof and for receiving information regarding authorization of the transaction; and

an output device connected to said processing unit for outputting the information regarding authorization of the transaction,

wherein the financial account identifier is a single-use financial account identifier containing information specific to the transaction.

16. An apparatus for verifying a financial account identifier, comprising:

a processing unit, said processing unit including a cryptographic processor;

a communications unit, connected to said processing unit, for transmitting and receiving information regarding the financial account identifier; and

a memory device connected to said processing unit, said memory device containing a private cryptographic key, a first data element, a second data element and a program, adapted to be executed by said processing unit, to receive a single-use financial account identifier, extract therefrom a third data element and a fourth data element, decrypt the third data element using the private cryptographic key and the fourth data element, compare the decrypted third data element with the first data element in a first comparison, compare the fourth data element with the second data element in a second comparison, and verify the received financial account identifier in accordance with the first comparison and the second comparison.

17. A method for generating a single-use financial account identifier, comprising the steps of:

providing a memory device containing a private cryptographic key, a first data element, and a second data element;

encrypting the first data element using the private cryptographic key, and the second data element;

modifying the second data element;

combining the encrypted first data element and the second data element to generate a single-use financial account identifier; and

displaying the single-use financial account identifier.

18. A method for facilitating a financial account transaction, comprising:

providing a processing unit;

inputting a financial account identifier to said processing unit;

transmitting the financial account identifier for verification thereof;

receiving information regarding authorization of the transaction based on said verification; and

outputting the information regarding authorization of the transaction,

wherein the financial account identifier is a single-use financial account identifier containing information specific to the transaction.

19. A method for verifying a single-use financial account identifier, comprising the steps of:

providing a memory device containing a private cryptographic key, a first data element and a second data element;

receiving said single-use financial account identifier;

extracting from said single-use financial account identifier a third data element and a fourth data element;

decrypting the third data element using the private cryptographic key and the fourth data element;

comparing the decrypted third data element with the first data element in a first comparison;

comparing the fourth data element with the second data element in a second comparison; and

verifying said single-use financial account identifier in accordance with the first comparison and the second comparison.

20. A device for providing a single-use financial account identifier, said device comprising:

a memory storing data representing a plurality of predetermined single-use financial account identifiers, data representing a status for each of said plurality of predetermined single-use financial account identifiers, and data representing a pointer to one of said plurality of predetermined single-use financial account identifiers;

an output device for presenting said single-use financial account identifier; and

a processor coupled to said memory and to said output device, said processor being configured to identify said single-use financial account identifier based on said data representing a pointer, said processor being further configured to transmit a signal to said output device to present said single-use financial account identifier.

21. A device according to claim 20, further comprising an input device adapted to transmit an input signal representing a request to present said single-use financial account identifier, wherein said processor is coupled to said input device and said processor is further configured to receive said input signal from said input device.

22. A device according to claim 20, wherein said processor is further configured to update said data representing a pointer and to update said data representing a status.

23. An apparatus for verifying a single-use financial account identifier, comprising:

a processing unit;

a communications unit, connected to said processing unit, for transmitting and receiving information regarding said single-use financial account identifier; and

a memory device connected to said processing unit, said memory device containing data representing a plurality of predetermined single-use financial account identifiers, data representing a status for each of said plurality of predetermined single-use financial account identifiers, and a program, adapted to be executed by said processing unit, to receive said single-use financial account identifier, compare said single-use financial account identifier with each of said plurality of predetermined single-use financial account identifiers to identify one predetermined single-use financial account identifier matching said single-use financial account identifier, and verify said single-use financial account identifier in accordance with said comparison and the data representing the status of said one predetermined single-use financial account identifier.

24. A method for providing a single-use financial account identifier, comprising the steps of:

providing a memory storing data representing a plurality of predetermined single-use financial account identifiers, data representing a status for each of said plurality of predetermined single-use financial account identifiers, and data representing a pointer to one of said plurality of predetermined single-use financial account identifiers;

identifying said single-use financial account identifier based on said data representing a pointer; and

transmitting a signal to an output device to present said single-use financial account identifier.

25. A method for verifying a single-use financial account identifier, comprising the steps of:

providing a memory device containing data representing a plurality of predetermined single-use financial account identifiers and data representing a status for each of said plurality of predetermined single-use financial account identifiers;

receiving said single-use financial account identifier;

comparing said single-use financial account identifier with said plurality of predetermined single-use financial account identifiers to identify one predetermined single-use financial account identifier matching said single-use financial account identifier; and

verifying said single-use financial account identifier in accordance with said comparison and the data representing the status of said one predetermined single-use financial account identifier.

ABSTRACT OF THE DISCLOSURE

A device for facilitating financial account transactions is described which includes a processing unit including a cryptographic processor. The device also includes an input unit, a display unit and a memory device connected to the processing unit. The memory device contains a private cryptographic key, a first data element and a second data element. The processing unit encrypts the first data element using the private cryptographic key and the second data element, modifies the second data element, combines the encrypted first data element and the second data element to generate a single-use financial account identifier, and displays the single-use financial account identifier. This identifier is then transmitted to a central processor for authorization of the transaction. The central processor extracts and decrypts data elements from the transmitted identifier using the private cryptographic key, compares those data elements with data elements stored in a memory, and verifies the single-use financial account identifier in accordance with the comparison.

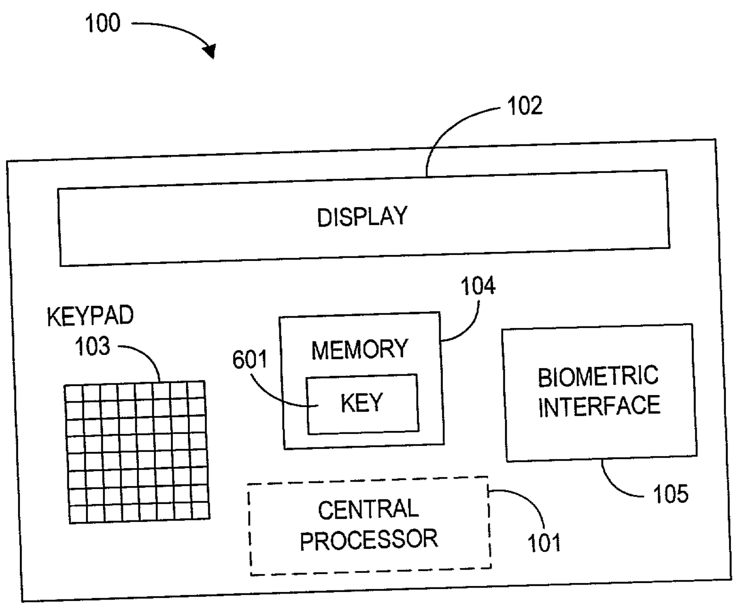
100
102
DISPLAY
KEYPAD
103
104
601
MEMORY
KEY
BIOMETRIC
INTERFACE
CENTRAL
PROCESSOR
101
105

FIG. 1

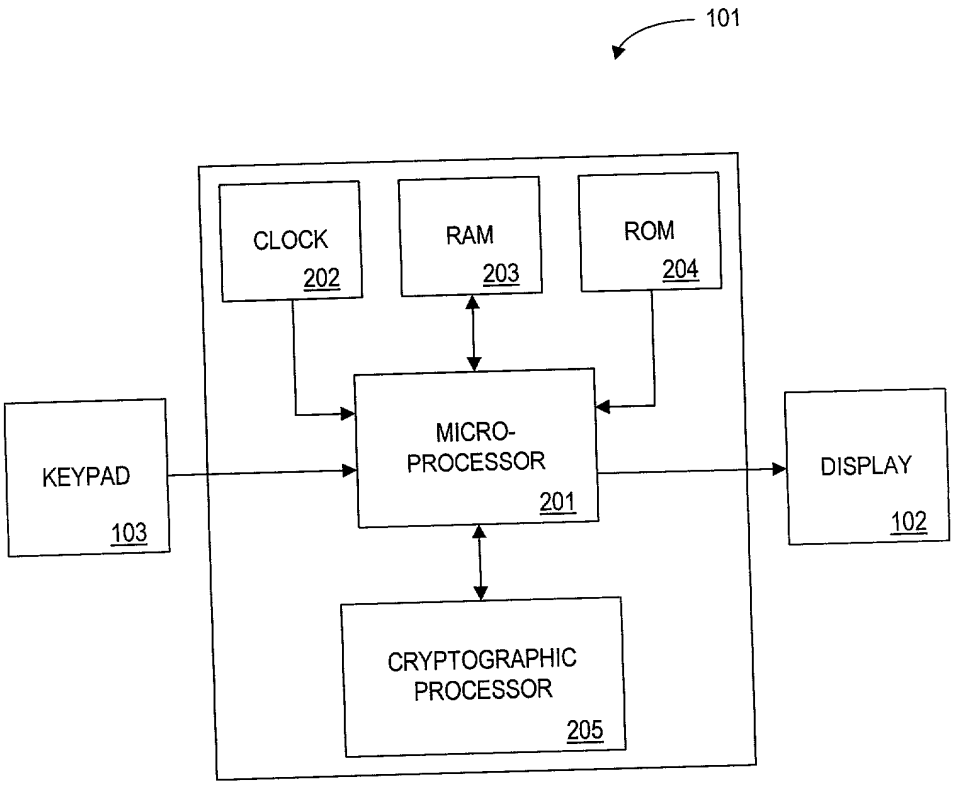
101
CLOCK
202
RAM
203
ROM
204
KEYPAD
103
MICRO-
PROCESSOR
201
DISPLAY
102
CRYPTOGRAPHIC
PROCESSOR
205

FIG. 2

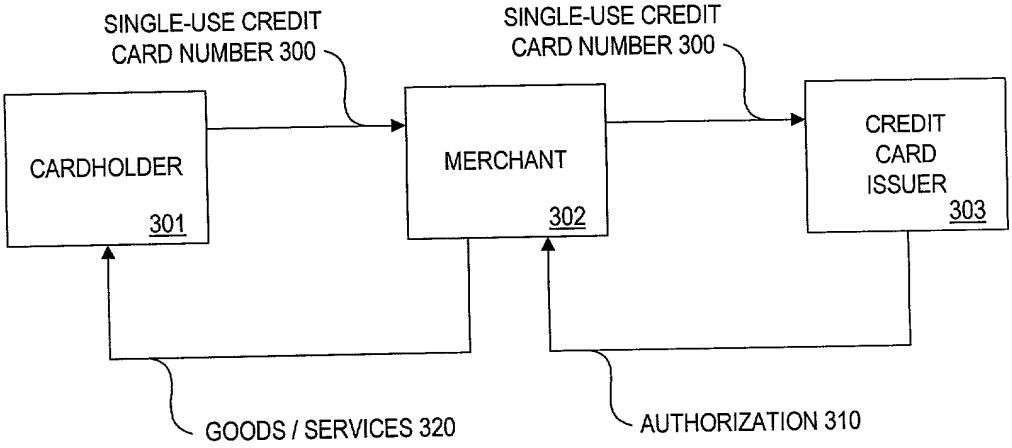

FIG. 3A

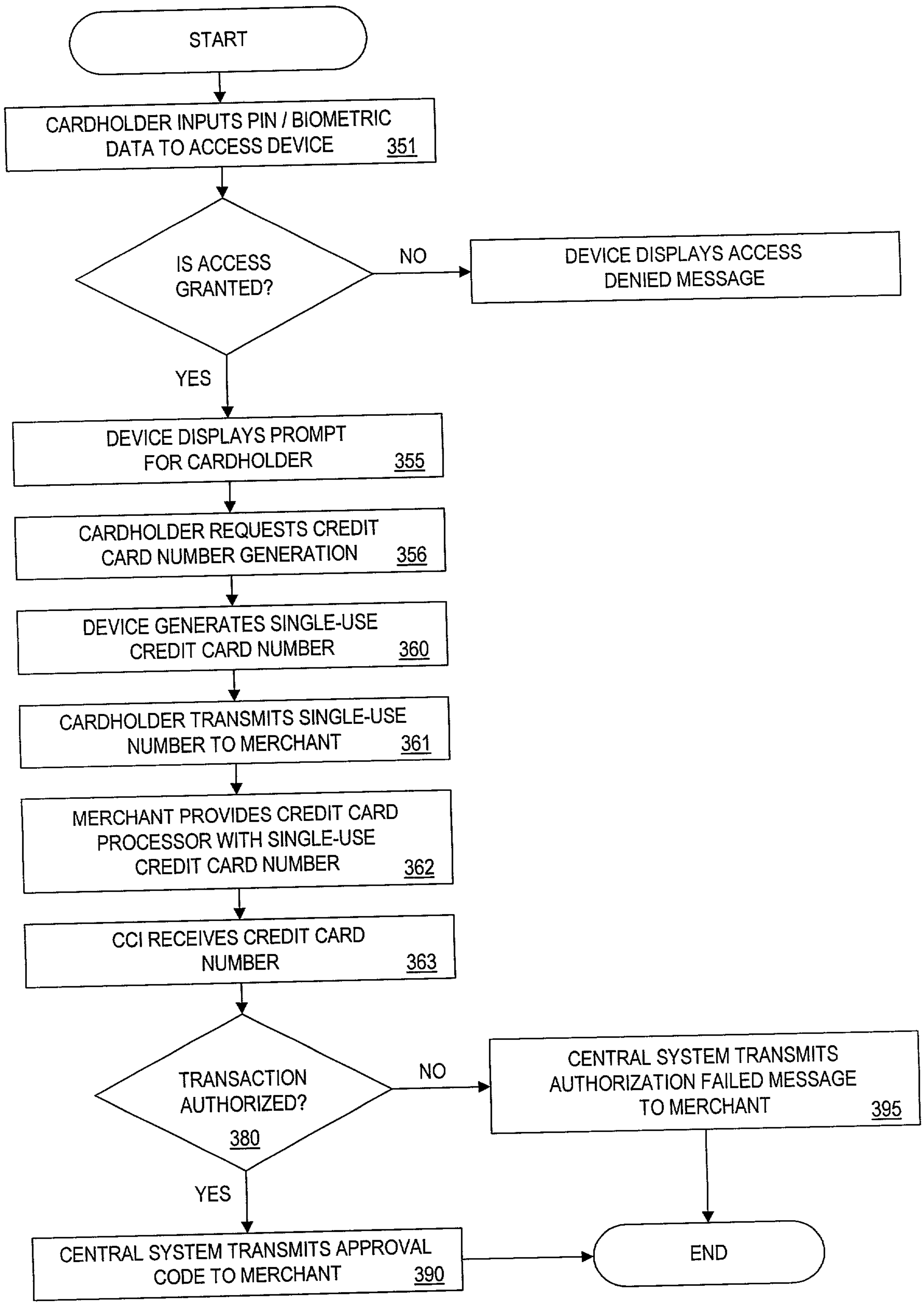
START
CARDHOLDER INPUTS PIN / BIOMETRIC DATA TO ACCESS DEVICE 351
IS ACCESS GRANTED?
NO
DEVICE DISPLAYS ACCESS DENIED MESSAGE
YES
DEVICE DISPLAYS PROMPT FOR CARDHOLDER 355
CARDHOLDER REQUESTS CREDIT CARD NUMBER GENERATION 356
DEVICE GENERATES SINGLE-USE CREDIT CARD NUMBER 360
CARDHOLDER TRANSMITS SINGLE-USE NUMBER TO MERCHANT 361
MERCHANT PROVIDES CREDIT CARD PROCESSOR WITH SINGLE-USE CREDIT CARD NUMBER 362
CCI RECEIVES CREDIT CARD NUMBER 363
TRANSACTION AUTHORIZED? 380
NO
CENTRAL SYSTEM TRANSMITS AUTHORIZATION FAILED MESSAGE TO MERCHANT 395
YES
CENTRAL SYSTEM TRANSMITS APPROVAL CODE TO MERCHANT 390
END

FIG. 3B

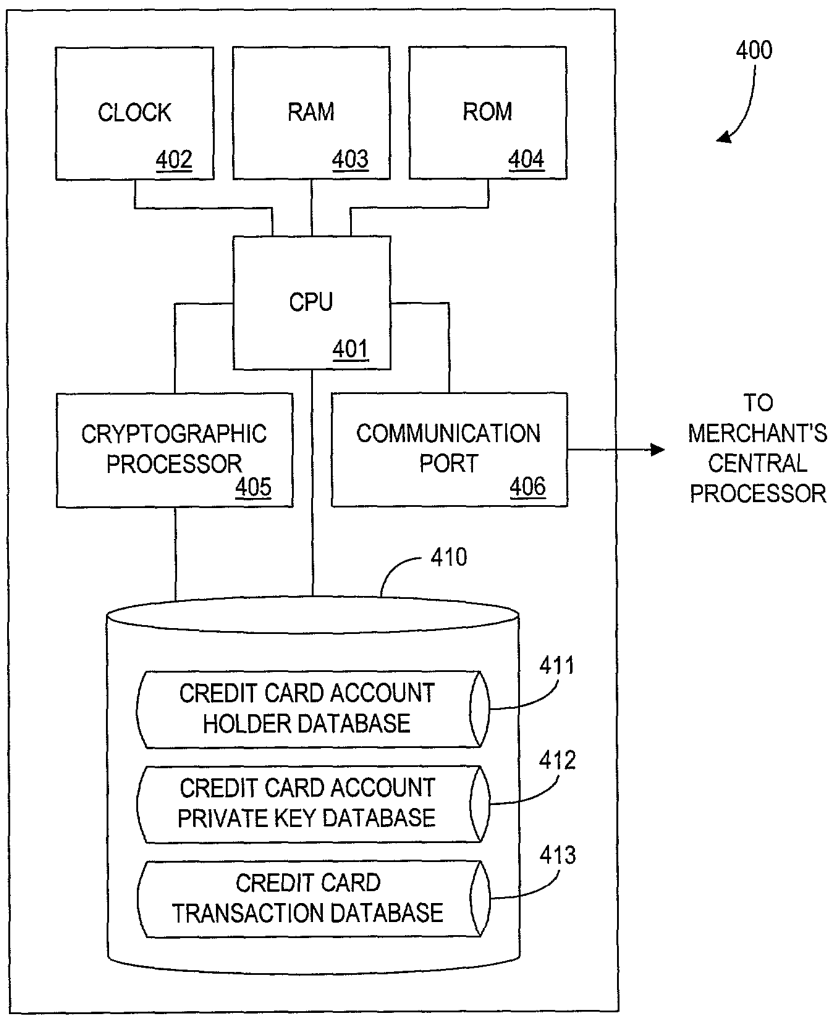
400
CLOCK
402
RAM
403
ROM
404
CPU
401
CRYPTOGRAPHIC
PROCESSOR
405
COMMUNICATION
PORT
406
TO
MERCHANT'S
CENTRAL
PROCESSOR
410
CREDIT CARD ACCOUNT
HOLDER DATABASE
411
CREDIT CARD ACCOUNT
PRIVATE KEY DATABASE
412
CREDIT CARD
TRANSACTION DATABASE
413

FIG. 4

411

CARDHOLDER ACCOUNT NUMBER 501	NAME 502	ADDRESS 503	PHONE NUMBER 504	TOTAL CREDIT LINE 505	AVAILABLE CREDIT LINE 506	EXPIRATION DATE 507
2222-3333-4444-5555	TIM JOHNSON	99 MAIN ST. HOMETOWN, CT 22222	(333) 444-5555	$2,000	$1,233	05/98
9999-8888-7777-6666	SUE MARVIN	10 CENTER ST. ROCKPORT, NJ 99999	(999) 111-2222	$3,500	$3,500	08/99

FIG. 5

412

CARDHOLDER PRIVATE KEY 601	CARDHOLDER ACCOUNT NUMBER 501	NONCE 602
1100010101110	2222-3333-4444-5555	1011011100011010
1000011111101	9999-8888-7777-6666	0111011110010100

FIG. 6

413

CARDHOLDER ACCOUNT NUMBER 501	EXPIRATION DATE 507	TRANSACTION AMOUNT 702	MERCHANT IDENTIFICATION NUMBER 703	INITIALIZATION VARIABLE 704
2222-3333-4444-5555	05/98	$23.98	123456	27
9999-8888-7777-6666	08/99	$56.34	654321	96

FIG. 7

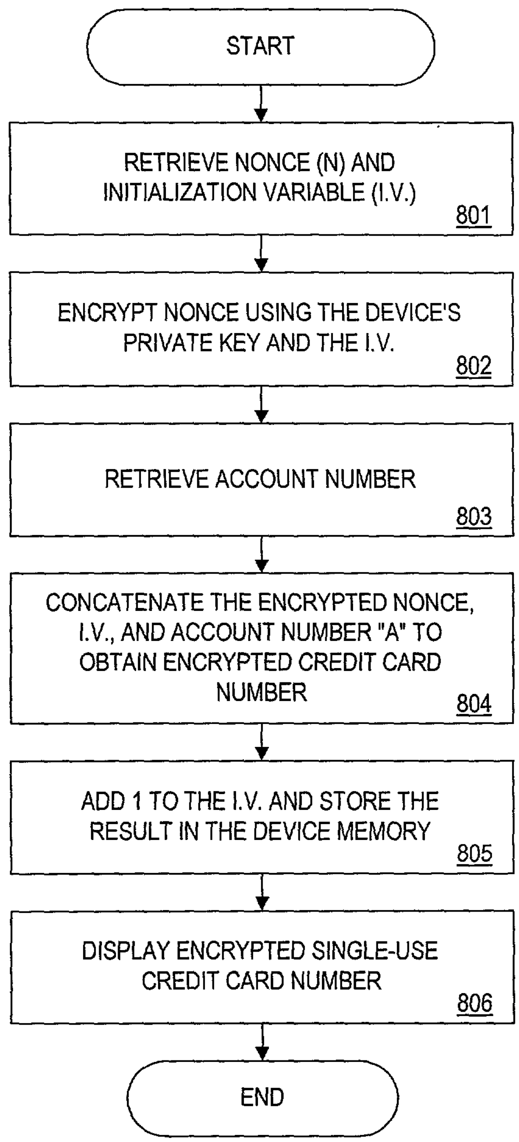
START
RETRIEVE NONCE (N) AND INITIALIZATION VARIABLE (I.V.)
801
ENCRYPT NONCE USING THE DEVICE'S PRIVATE KEY AND THE I.V.
802
RETRIEVE ACCOUNT NUMBER
803
CONCATENATE THE ENCRYPTED NONCE, I.V., AND ACCOUNT NUMBER "A" TO OBTAIN ENCRYPTED CREDIT CARD NUMBER
804
ADD 1 TO THE I.V. AND STORE THE RESULT IN THE DEVICE MEMORY
805
DISPLAY ENCRYPTED SINGLE-USE CREDIT CARD NUMBER
806
END

FIG. 8

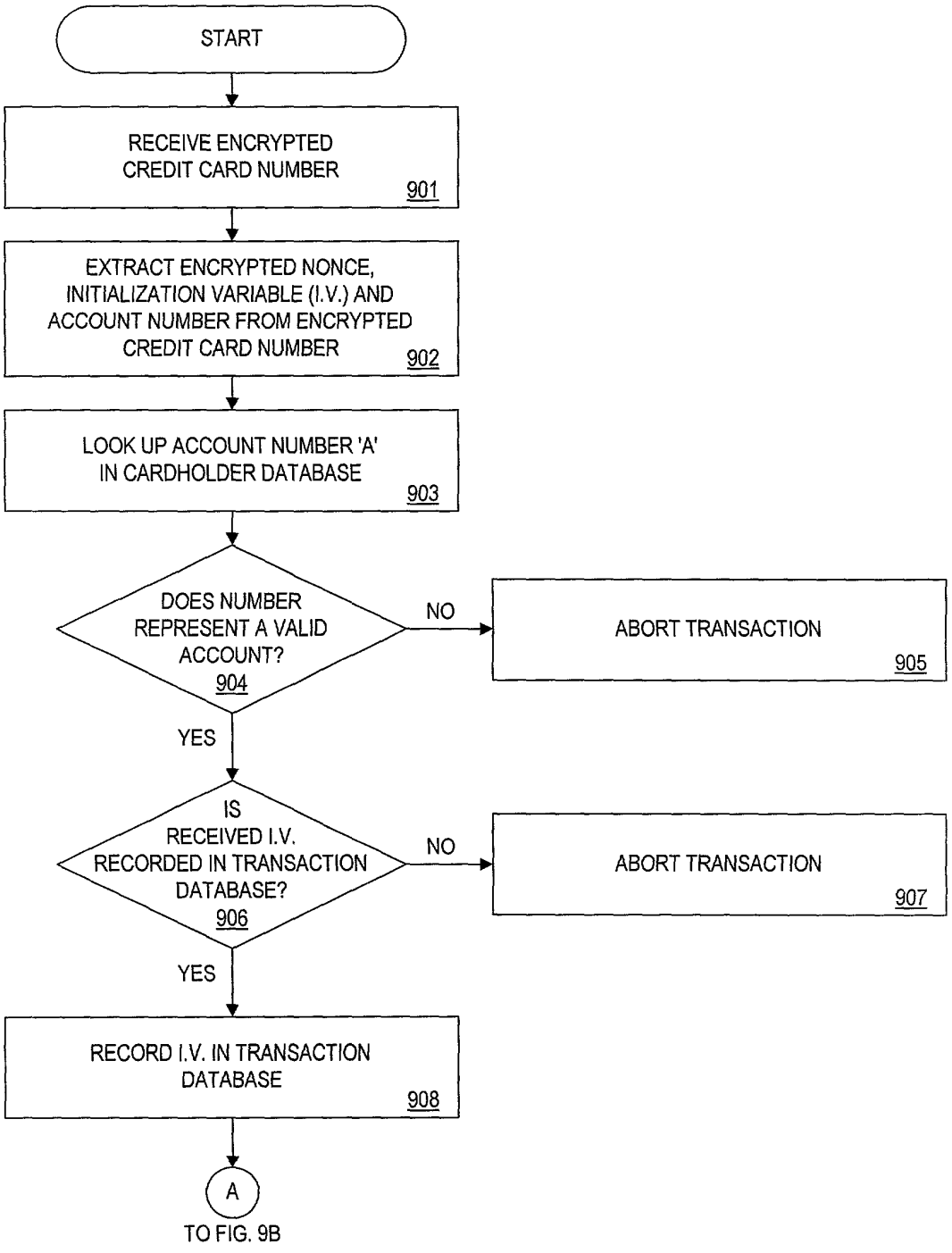
START
RECEIVE ENCRYPTED CREDIT CARD NUMBER
901
EXTRACT ENCRYPTED NONCE, INITIALIZATION VARIABLE (I.V.) AND ACCOUNT NUMBER FROM ENCRYPTED CREDIT CARD NUMBER
902
LOOK UP ACCOUNT NUMBER 'A' IN CARDHOLDER DATABASE
903
DOES NUMBER REPRESENT A VALID ACCOUNT?
904
NO
ABORT TRANSACTION
905
YES
IS RECEIVED I.V. RECORDED IN TRANSACTION DATABASE?
906
NO
ABORT TRANSACTION
907
YES
RECORD I.V. IN TRANSACTION DATABASE
908
A
TO FIG. 9B

FIG. 9A

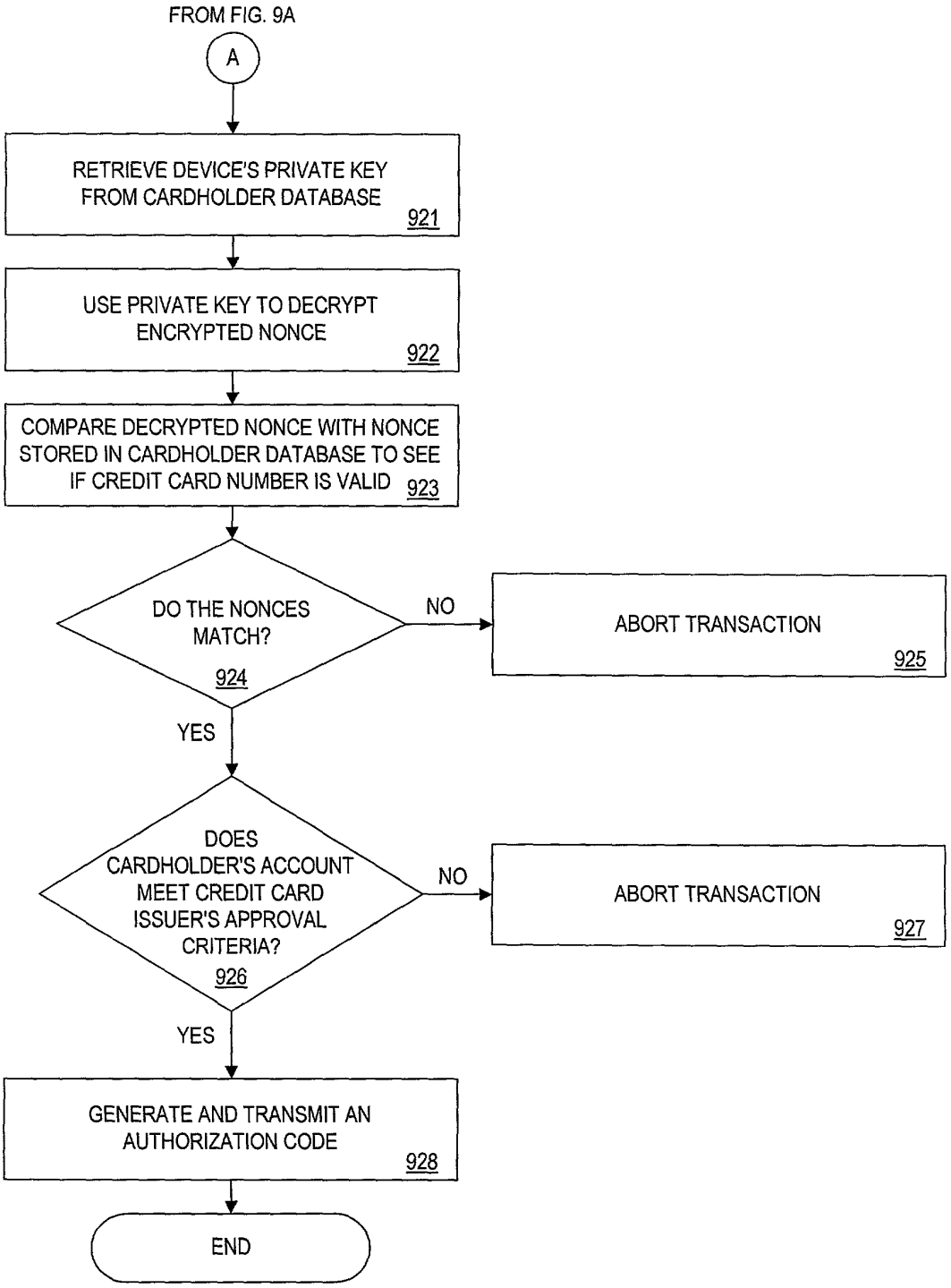
FROM FIG. 9A
A
RETRIEVE DEVICE'S PRIVATE KEY FROM CARDHOLDER DATABASE
921
USE PRIVATE KEY TO DECRYPT ENCRYPTED NONCE
922
COMPARE DECRYPTED NONCE WITH NONCE STORED IN CARDHOLDER DATABASE TO SEE IF CREDIT CARD NUMBER IS VALID
923
DO THE NONCES MATCH?
924
NO
ABORT TRANSACTION
925
YES
DOES CARDHOLDER'S ACCOUNT MEET CREDIT CARD ISSUER'S APPROVAL CRITERIA?
926
NO
ABORT TRANSACTION
927
YES
GENERATE AND TRANSMIT AN AUTHORIZATION CODE
928
END

FIG. 9B

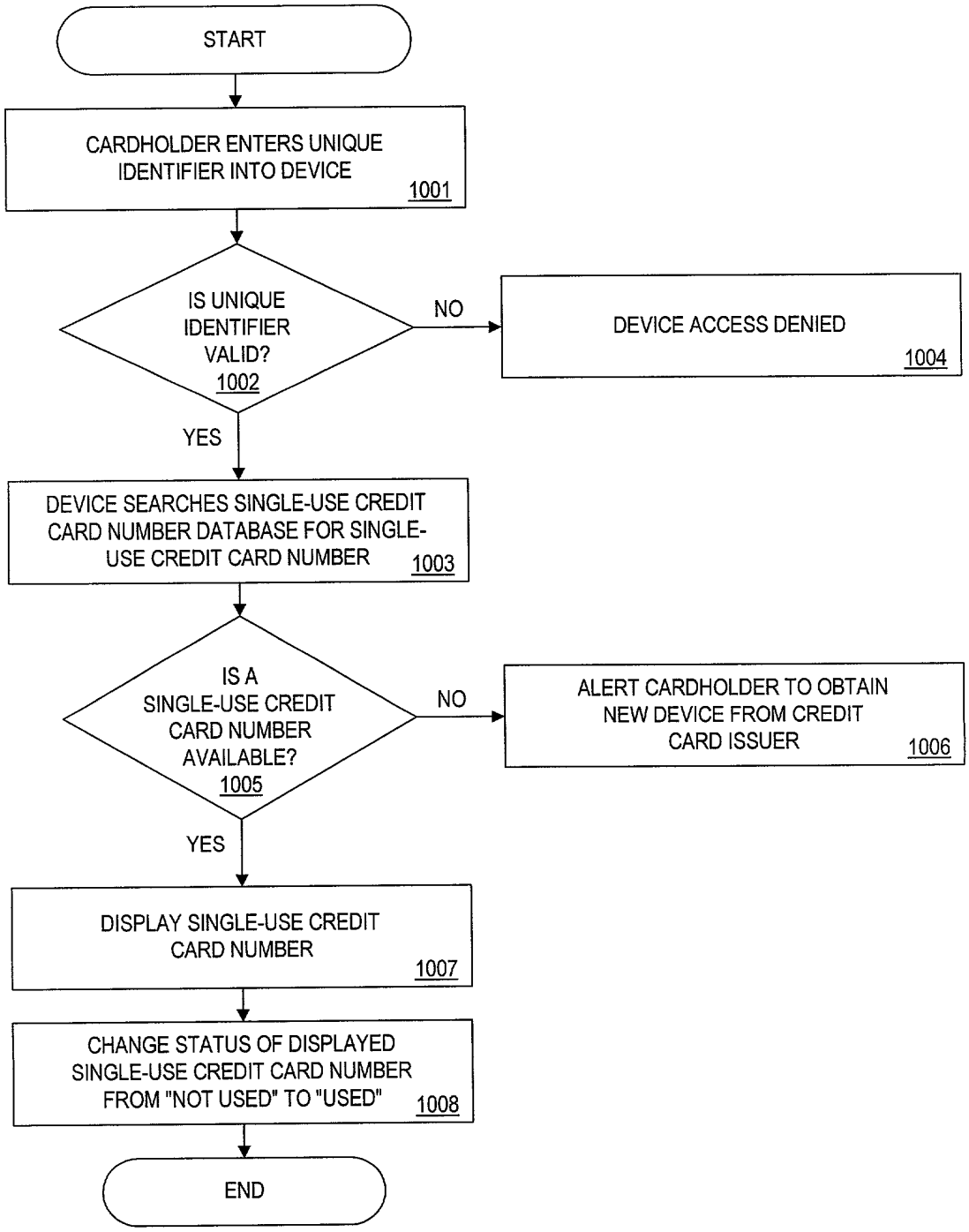
START
CARDHOLDER ENTERS UNIQUE IDENTIFIER INTO DEVICE
1001
IS UNIQUE IDENTIFIER VALID?
1002
NO
DEVICE ACCESS DENIED
1004
YES
DEVICE SEARCHES SINGLE-USE CREDIT CARD NUMBER DATABASE FOR SINGLE-USE CREDIT CARD NUMBER
1003
IS A SINGLE-USE CREDIT CARD NUMBER AVAILABLE?
1005
NO
ALERT CARDHOLDER TO OBTAIN NEW DEVICE FROM CREDIT CARD ISSUER
1006
YES
DISPLAY SINGLE-USE CREDIT CARD NUMBER
1007
CHANGE STATUS OF DISPLAYED SINGLE-USE CREDIT CARD NUMBER FROM "NOT USED" TO "USED"
1008
END

FIG. 10

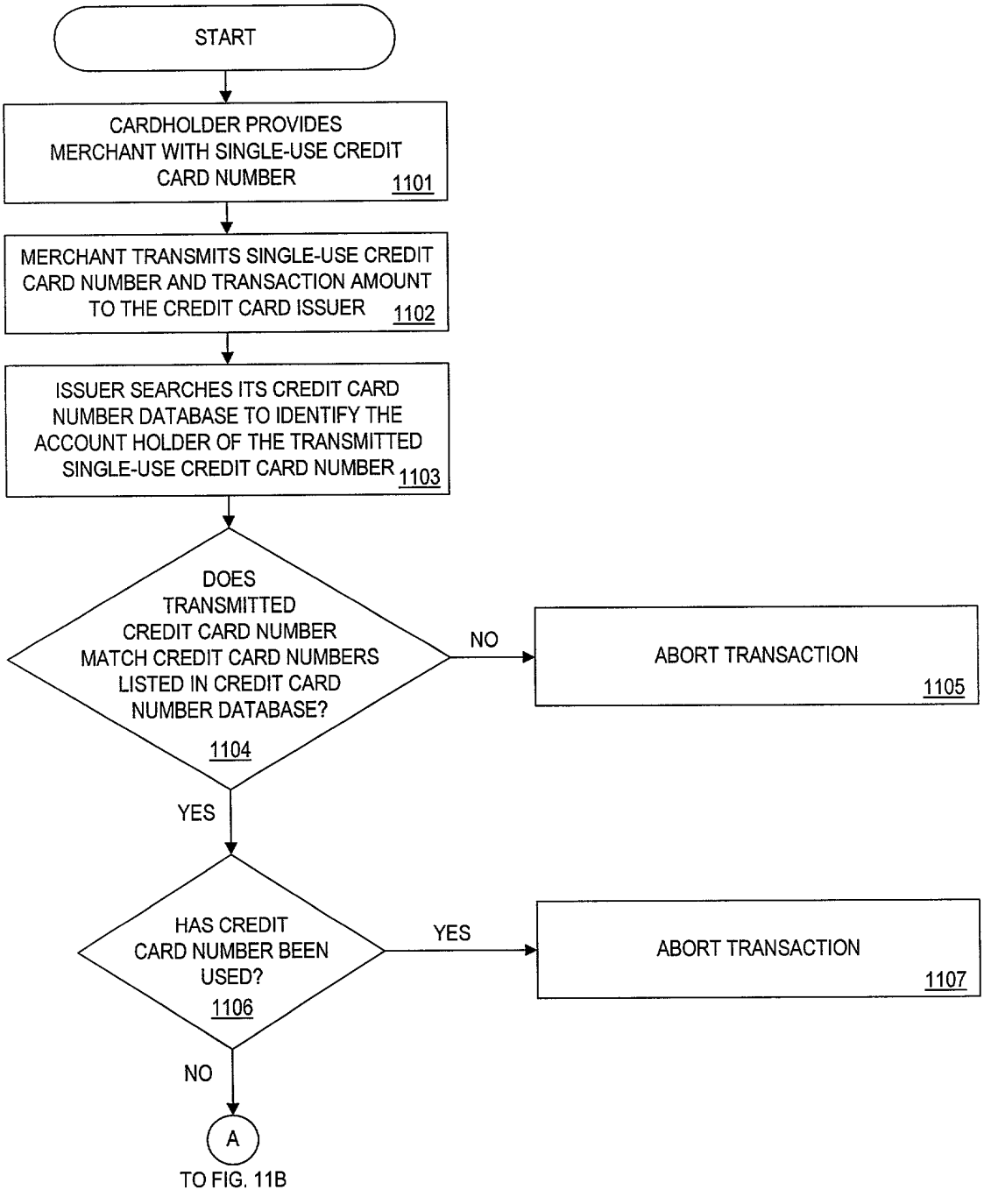
START
CARDHOLDER PROVIDES MERCHANT WITH SINGLE-USE CREDIT CARD NUMBER 1101
MERCHANT TRANSMITS SINGLE-USE CREDIT CARD NUMBER AND TRANSACTION AMOUNT TO THE CREDIT CARD ISSUER 1102
ISSUER SEARCHES ITS CREDIT CARD NUMBER DATABASE TO IDENTIFY THE ACCOUNT HOLDER OF THE TRANSMITTED SINGLE-USE CREDIT CARD NUMBER 1103
DOES TRANSMITTED CREDIT CARD NUMBER MATCH CREDIT CARD NUMBERS LISTED IN CREDIT CARD NUMBER DATABASE? 1104
NO
ABORT TRANSACTION 1105
YES
HAS CREDIT CARD NUMBER BEEN USED? 1106
YES
ABORT TRANSACTION 1107
NO
A
TO FIG. 11B

FIG. 11A

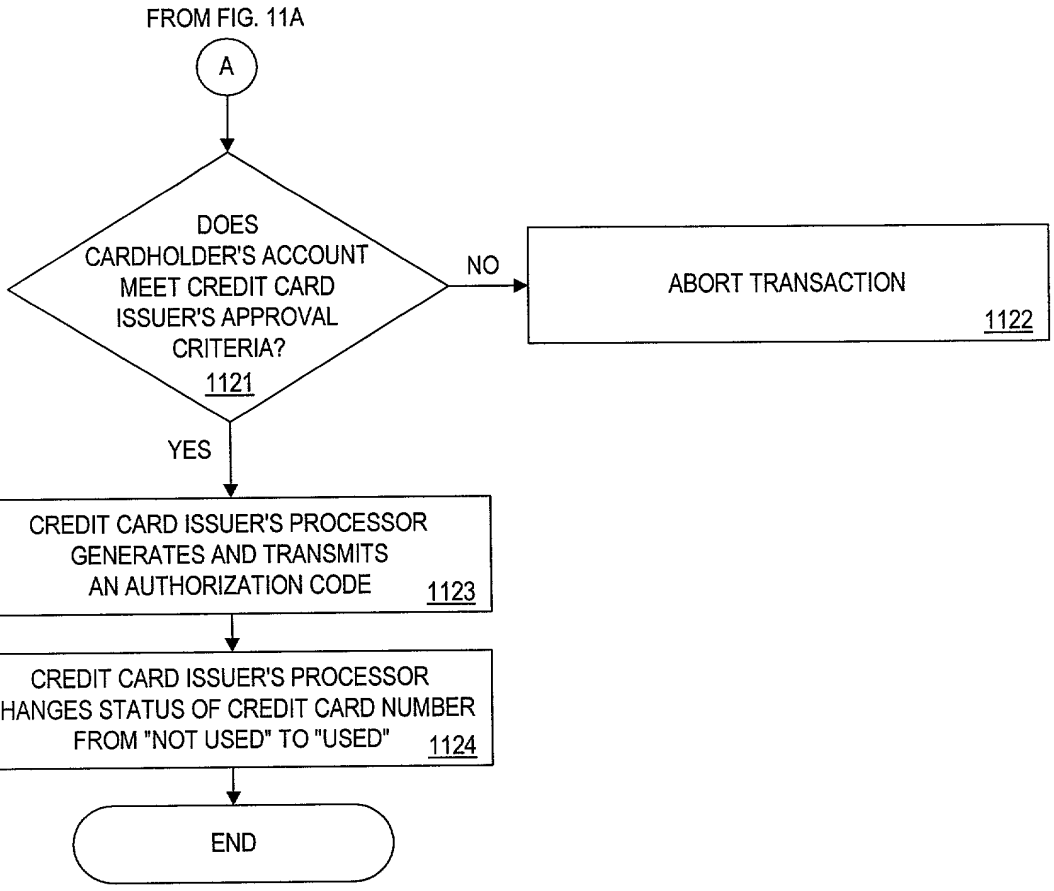
FROM FIG. 11A
A
DOES CARDHOLDER'S ACCOUNT MEET CREDIT CARD ISSUER'S APPROVAL CRITERIA?
1121
NO
ABORT TRANSACTION
1122
YES
CREDIT CARD ISSUER'S PROCESSOR GENERATES AND TRANSMITS AN AUTHORIZATION CODE
1123
CREDIT CARD ISSUER'S PROCESSOR CHANGES STATUS OF CREDIT CARD NUMBER FROM "NOT USED" TO "USED"
1124
END

FIG. 11B

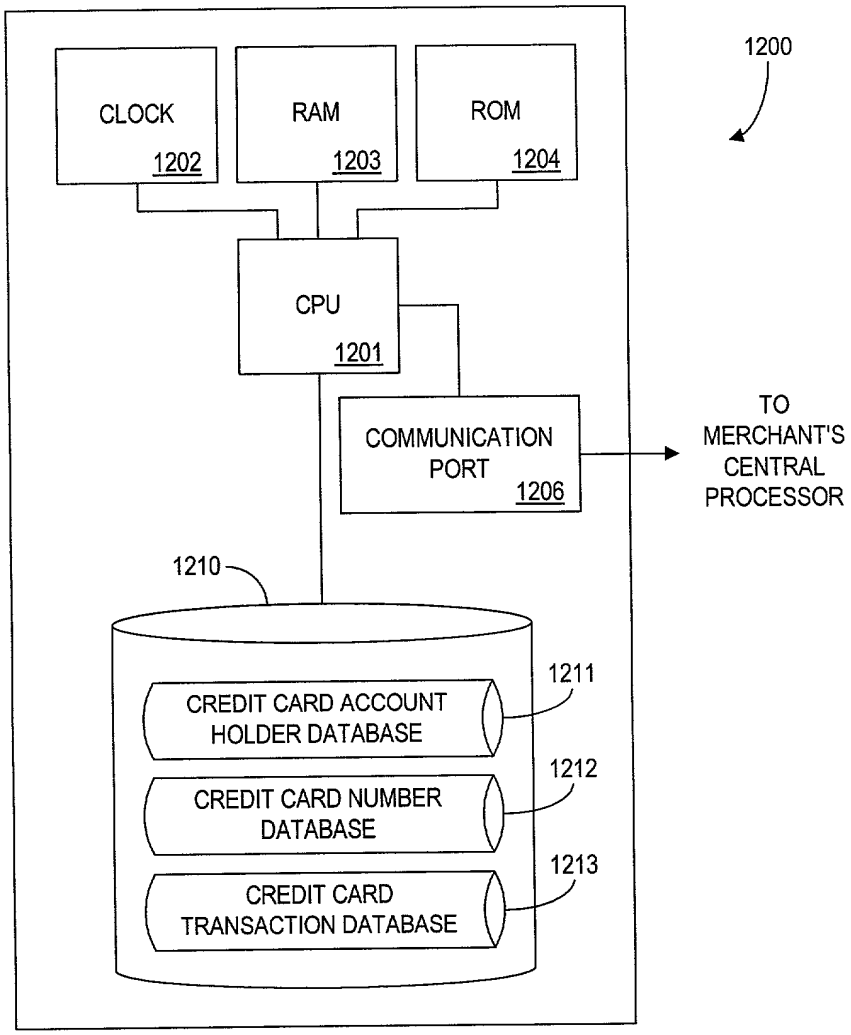
1200
CLOCK
1202
RAM
1203
ROM
1204
CPU
1201
COMMUNICATION PORT
1206
TO MERCHANT'S CENTRAL PROCESSOR
1210
1211
CREDIT CARD ACCOUNT HOLDER DATABASE
1212
CREDIT CARD NUMBER DATABASE
1213
CREDIT CARD TRANSACTION DATABASE

FIG. 12

CARDHOLDER ACCOUNT NUMBER 501	CARDHOLDER NAME 502	CREDIT CARD NUMBER 1301	STATUS 1302
2222-3333-4444-5555	TIM JOHNSON	3122-2222-3333-6644	USED
		3122-1222-3333-7697	NOT USED
		⋮	⋮
		3122-1222-3394-4181	NOT USED
9999-8888-7777-6666	SUE MARVIN	1454-8000-3366-7171	USED
		1454-8000-3366-7172	USED
		⋮	⋮
		1454-8000-3989-6097	NOT USED

FIG. 13

1213

CARDHOLDER ACCOUNT NUMBER 501	EXPIRATION DATE 507	TRANSACTION AMOUNT 702	MERCHANT IDENTIFICATION NUMBER 703
2222-3333-4444-5555	05/22/98	$23.98	123456
9999-8888-7777-6666	08/01/99	$56.34	654321

FIG. 14

COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

(Page 1)

COPY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER, the specification of which [X] is attached hereto [ ] was filed on _____ _ as United States Application No. or PCT International Application No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: Joseph M. Fitzpatrick (Registration No. 17,398), Lawrence F. Scinto (Registration No. 18,973), William J. Brunet (Registration No. 20,452), Robert L. Baechtold (Registration No. 20,860), John A. O'Brien (Registration No. 24,367), John A. Krause (Registration No. 24,613), Henry J. Renk (Registration No. 25,499), Peter Saxon (Registration No. 24,947), Anthony M Zupcic (Registration No. 27,276), Charles P. Baker (Registration No. 26,702), Stevan J. Bosses (Registration No. 22,291), Edward E. Vassallo (Registration No. 29,117), Ronald A. Clayton (Registration No. 26,718), Lawrence A. Stahl (Registration No. 30,110), Laura A. Bauer (Registration No. 29,767), Leonard P. Diana (Registration No. 29,296), David M. Quinlan (Registration No. 26,641), Nicholas N. Kallas (Registration No. 31,530), William M. Wannisky (Registration No. 28,373), Lawrence S. Perry (Registration No. 31,865), Robert H. Fischer (Registration No. 30,051), Christopher Philip Wrist (Registration No. 32,078), Gary M. Jacobs (Registration No. 28,861), Michael K. O'Neill (Registration No. 32,622), Bruce C. Haas (Registration No. 32,734), Scott K. Reed (Registration No. 32,433), Scott D. Malpede (Registration No. 32,533), Fredrick M. Zullow (Registration No. 32,452), Richard P. Bauer (Registration No. 31,588), Warren E. Olsen (Registration No. 27,290), Abigail F. Cousins (Registration No. 29,292), Steven E. Warner (Registration No. 33,326), Thomas J. O'Connell (Registration No. 33,202), Penina Wollman (Registration No. 30,816), David L. Schaeffer (Registration No. 32,716), Jack S. Cubert (Registration No. 24,245), Mark A. Williamson (Registration No. 33,628), Jean K. Dudek (Registration No. 30,938), Raymond R. Mandra (Registration No. 34,382), Dominick A. Conde (Registration No. 33,856), Pasquale A. Razzano (Reg. No. 25,512), John W. Behringer (Registration No. 23,086), Robert C. Kline (Registration No. 17,739), Mark J. Itri (Registration No. 36,171), Michael P. Sandonato (Registration No. 35,345), Jack M. Arnold (Registration No. 25,823), John D. Carlin (Registration No. 37,292), Daniel S. Glueck (Registration No. 37,838), Joseph W. Ragusa (Registration No. 38,586), Brian L. Klock (Registration No. 36,570), Anne M. Maher (Registration No. 38,231), William J. Zak, Jr. (Registration No. 38,668), Thomas D. Pease (Registration No. 35,317), Bruce M. Wexler (Registration No. 35,409), Robert S. Mayer (Registration No. 38,544), Errol B. Taylor (Registration No. 39,853), Matthew J. Golden (Registration No. 35,161), Sean W. O'Brien (Registration No. 37,689), Dolores A. Moro-Grossman (Registration No. 33,972), T. Thomas Gellenthien (Registration No. 39,683), Douglas Sharrott (Registration No. 39,832), Gordon F. Sieckmann (Registration No. 28,667), Jay H. Anderson (Registration No. 38,371), Jeffrey L. Brandt (Registration No. 31,490) and Robert R. Lech (Registration No. 37,169).

Address all correspondence to:

FITZPATRICK, CELLA, HARPER & SCINTO
277 Park Avenue
New York, N.Y. 10172
Telephone No. (212) 758-2400

COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION
(Page 2)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First Inventor JAY S. WALKER
Inventor's signature _____
Date 8/26/97 Citizen/Subject of United States
Residence 124 Spectacle Lane
Ridgefield, Connecticut 06877
Post Office Address c/o Walker Digital, 5 High Ridge Park
Stamford, Connecticut 06905

Full Name of Second Joint Inventor BRUCE SCHNEIER
Second Inventor's signature _____
Date 8/25/97 Citizen/Subject of United States
Residence 101 E. Minnehaha Parkway
Minneapolis, Minnesota 55419
Post Office Address c/o Walker Digital, 5 High Ridge Park
Stamford, Connecticut 06905

Full Name of Third Joint Inventor SANJAY K. JINDAL
Third Inventor's signature _____
Date 8/26/97 Citizen/Subject of India
Residence 52 Village Walk
Wilton, Connecticut 06897
Post Office Address c/o Walker Digital, 5 High Ridge Park
Stamford, Connecticut 06905

Full Name of Fourth Joint Inventor DANIEL E. TEDESCO
Fourth Inventor's signature _____
Date 8/26/97 Citizen/Subject of United States
Residence 88 Barn Hill Road
Monroe, Connecticut 06468
Post Office Address c/o Walker Digital, 5 High Ridge Park
Stamford, Connecticut 06905
F501\A572551

COPY

Attorney Docket No.: WD2-96-059

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Jay S. Walker et al.		
For:	METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER	Examiner:	Demetra R. Smith
Serial No.:	08/919,339	Group Art Unit:	2764
Filing Date:	August 18, 1997	Docket No.:	WD2-96-059

Assistant Commissioner of Patents
Washington, D.C. 20231

REVOCATION AND APPOINTMENT OF POWER OF ATTORNEY

Sir:

Walker Asset Management Limited Partnership, the sole assignee and owner of the entire right, title and interest in the above-identified patent application, hereby revokes all previous powers of attorney and hereby appoints Dean Alderucci (PTO Reg. No. 40,484), Patrick J. Buckley (PTO Reg. No. 40,928), Steven M. Santisi (PTO Reg. No. 40,157), and Kurt M. Maschoff (PTO Reg. No. 38,235) as attorneys of record, all of Walker Digital Corporation located at One High Ridge Park, Stamford, Connecticut 06905-1326, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all written correspondence to:

Walker Digital Corporation
One High Ridge Park
Stamford, CT 06905-1326
Phone (203) 905-6500
Fax (203) 595-8266

Certificate Under 37 C.F.R. § 3.73(b)

Walker Asset Management Limited Partnership, a limited partnership organized and existing under the laws of the state of Connecticut, certifies that it is the assignee of the entire right, title and interest in the patent application identified above by virtue of either:

A. [X] An Assignment from the inventor(s) of the patent application identified above. The assignment was recorded in the U.S. Patent and Trademark Office on August 28, 1997, at Reel 8696, Frame 0332, or for which a copy thereof is attached.

B. [ ] A chain of title from the inventor(s) of the patent application identified above to the current assignee as shown below:

1. From:_____ To:_____
The document was recorded in the Patent and Trademark Office at Reel_____, Frame_____, or for which a copy thereof is attached.

2. From:_____ To:_____
The document was recorded in the Patent and Trademark Office at Reel_____, Frame_____, or for which a copy thereof is attached.

3. From:_____ To:_____
The document was recorded in the Patent and Trademark Office at Reel_____, Frame_____, or for which a copy thereof is attached.

4. From:_____ To:_____
The document was recorded in the Patent and Trademark Office at Reel_____, Frame_____, or for which a copy thereof is attached.

C. [ ] Copies of the assignments or other documents in the chain of title are attached.

The undersigned has reviewed all the documents in the chain of title of the patent application identified above and to the best of undersigned's knowledge and belief, title is in the assignee identified above.

The undersigned (whose title is supplied below) is empowered to act on behalf of the assignee.

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001, Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application identified above or any patent issuing thereon.

Walker Asset Management Limited Partnership

Dated: August 19, 1999

By_____
Jay S. Walker,
President of Walker Digital Corp. as General Partner of Walker Asset Management Limited Partnership